90

一种基于Rossler混沌序列的图像加密技术

05级2A班　刘晓彬　20052301203

指导老师：李军

摘要：一般而言，混沌是非线性动力学系统所特有的一种运动形式。混沌序列具有易生成、对初始条件强敏感性、可完全重现性以及整体的伪白噪声统计的特性等特点，同时混沌序列的离散映射序列也具有相似的特性。混沌序列在原理上只要增加迭代次数，设定初始值和结构参数，就可以提供数量众多、非相关和长周期的伪随机码。基于以上特性，给出了一种基于Rossler混沌序列的图像置乱加密算法：首先，以初始条件为密匙生成混沌序列N个值，然后按照排序置乱算法，对图像I逐行逐列进行置乱和加密，并对其解密。实验结果证明，该算法实现简单，且图像的解密结果对混沌序列的初始值有很强的依赖性，具有较高的安全性以及加密效果。

关键词：Rossler系统、混沌序列、置乱、排序变换、图像加密

An technology of Image Encryption Based on Rossler Chaotic Sequence

Class 2A　Grade 05　LIU Xiao-Bin　20052301203

Mentor ： LI Jun

Abstract: Generally speaking, chaos is a proper motion of non-linear dynamics system. Chaotic sequence has the characteristic of :easy to create、sensitive of initial condition、entire recur and holistic noisy digit. Synchronously, discrete mapped sequence of chaotic Sequence

has the same property. Chaotic sequence can create numerous of uncorrelative and long period of random code by enlarging iterative times and fix initial value. Basing on the properties above, here is a technology of image encryption algorithm Based on rossler chaotic sequence: Using initial condition as a key to make chaotic sequence of N value, according to transform of scrambling algorithm to scramble and encrypt the image by rows, and then disclose it. The result of experiment improves that this algorithm achieve easily, the disclosed effect greatly lies on the initial value of chaotic sequence, and it has high security as well as encrypted effect.

Key words: Rossler System、Chaotic Sequence、Scrambling、Transform of Taxis、Image Encryption

1、引言

随着计算机网络通信技术迅猛发展，数字媒体（包括数字音频、数字图像和数字视频）得到广泛应用，然而数字产品极易被非法拷贝和分发，如何在交流各种信息中进行版权保护、确保信息与保密性已成为时代产权保护和认证的核心问题。传统的加密技术具有一定的局限性，一般都具有一定的规律性，可破解的机会较大，它已不能很好地满足人们对版权信息安全性的要求。而基于混沌的图像置乱加密技术，因为混沌系统是一种复杂的非线性动力学系统，具有良好的伪随机特性、轨道的不可预测性、对初始状态及控制参数极端敏感等特性，使得这种技术具有足够大的密码空间及较高的保密性能，因此，它也成为近年来保密通信领域内的一项重大研究课题。

目前应用混沌的图像置乱方案一般都是先通过计算混沌模拟序列，再对其进行多值量化来生成置换地址码。由于对混沌模拟序列进行量化要求对混沌的轨道的概率分布有相当的了解，而正是混沌研究的难题之一，并且易受量化精度的影响，因此多值量化所得到置换地址码很难完全保持混沌固有的特性。图像置乱的要求是置乱后的图像应具有较低的可懂度，并能抗一定程度的破译攻击，而解密

后图像又能准确表达原始图像的内容。而在本文提出的置乱算法，其置换地址码的产生则不需要对混沌实值序列进行量化，而是通过排序变换直接由混沌模拟序列来产生。本文算法不仅仅减少了混沌映射迭代次数，并能很好地利用混沌的特性，同时由于混沌序列的初值敏感性和排序变换的强不规则性，这也增加了破译置乱图像的难度，提高了图像的安全性和加密效果。

2、 关于 Rossler 映射混沌系统

Rossler 方程组是非线性动力学中的一个非常著名的方程，在理论和实际中都有非常重要的价值。其定义如下：

$$\begin{cases} x' = -y - z \\ y' = x + ay \\ z' = b + z(x - c) \end{cases}$$

当固定参数 b=2 ，c=4，而参数 a 由小到大变化（如 $0 \le a \le 0.65$ ）时，方程的解也随着变化，而且 Rossler 映射会出现混沌状态。也就是说，由初始条件 x_0、y_0、z_0 在 rossler 映射的作用下所产生的序列 x_k、y_k、z_k，其中 k=0，1，2，… 是非周期的，混沌的，且对初始值非常敏感的。

下面为计算模拟 Rossler 系统情况：

建立函数 M 文件 rossler1.m，在其中用 x(1)表示 x，用 x(2)表示 y，用 x(3)表示 z：

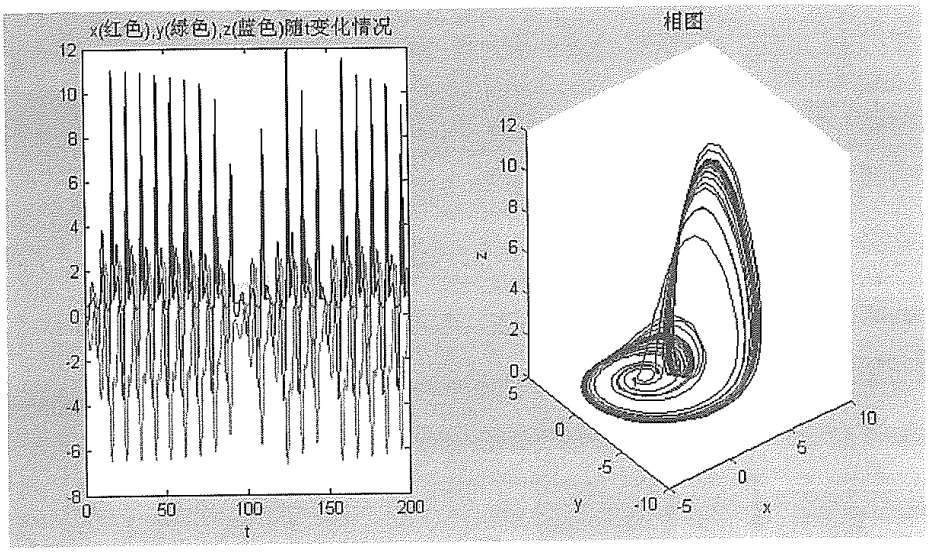
```
function r=rossler1(t,x)
global a; %定义全局变量 a
global b; %定义全局变量 b
global c; %定义全局变量 c
r=[-x(2)-x(3);x(1)+a*x(2);b+x(3)*(x(1)-c)]; %对 Rossler 方程组的定义
```

主程序文件：

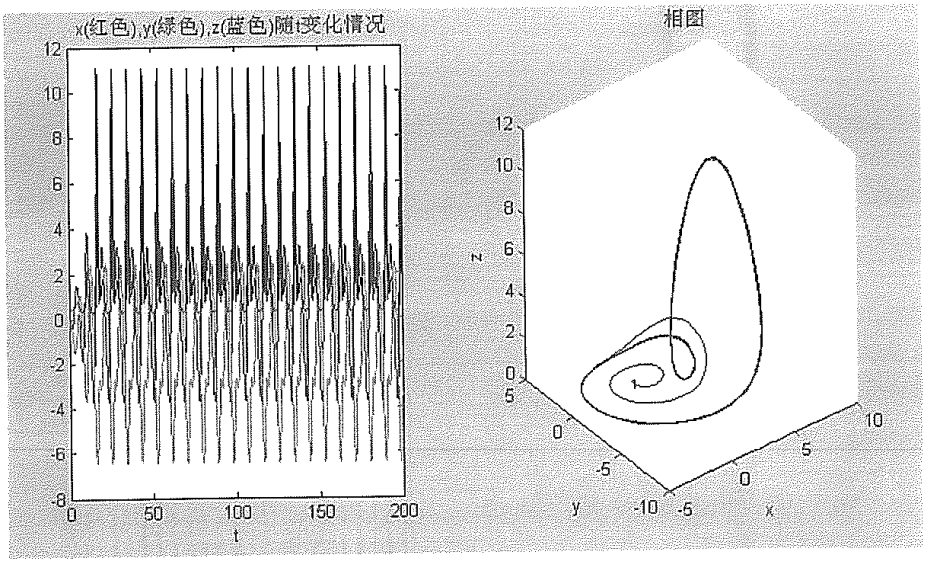
```
global a; %定义全局变量 a
global b; %定义全局变量 b
global c; %定义全局变量 c
b=2; %设定初值
c=4; %设定初值
t0=[0,200]; %建立循环开始迭代
for a=0.5 %给予 a 不同的初值
    [t,x]=ode45('rossler1',t0,[0,0,0]); %用 ode45 函数调用 rossler.m
    subplot(1,2,1); %在一个图像窗口中显示多个图形
        plot(t,x(:,1),'r',t,x(:,2),'g',t,x(:,3),'b'); %画图
        title('x(红色),y(绿色),z(蓝色)随 t 变化情况');xlabel('t');
%写出图像标题和注释
    subplot(1,2,2); %在一个图像窗口中显示多个图形
        plot3(x(:,1),x(:,2),x(:,3)) %画图
        title('相图');xlabel('x');ylabel('y');zlabel('z'); %写出
图像标题
    pause %停止
end %结束循环
```

用 Matlab 软件模拟 Rossler 系统的结果：

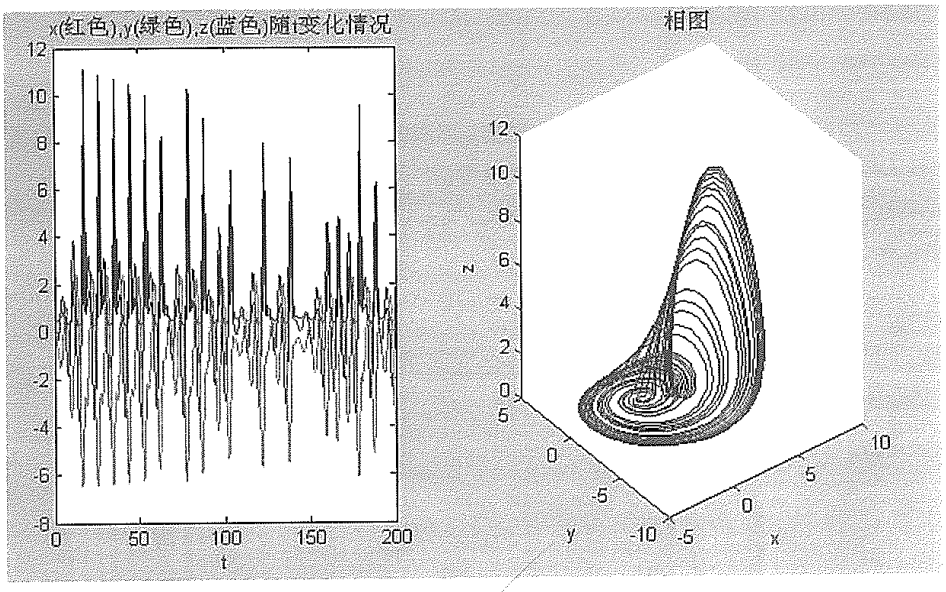
(1)、a=0.5



(2)、a=0.501



(3)a=0.499



从上面 a=0.5、a=0.501、a=0.499 得出的三个迭代图像表明：当初始值 a 改变很小的时候，运行后的结果就已经有很大的差别了，这说明了 Rossler 这个系统的混沌性，对其初值的敏感性，同时也说明了用它对图像进行加密的可行性和安全性。

3、 基于排序变换的混沌图像置乱算法

对于一个数字的灰度图像 I，其大小为 N×M,可以利用 Rossler 混沌迭代来产生混沌实值序列，然后通过下面描述的置乱算法即可对图像 I 逐行进行置乱和加密。

3.1 置乱算法

置乱算法步骤如下：

(1)、给定迭代初始值 x_1（相当于密匙）；

(2)、经 N-1 次混沌迭代运算得到混沌实值序列；$\{x_1, x_2, x_3, \cdots, x_n\}$；

(3)、通过排序变换，将实值序列集合$\{x_1, x_2, x_3, \cdots, x_n\}$中的 N 个值由小到大排序，形成有序序列；

（4）、确定混沌实值序列$\{x_1,x_2,x_3,\cdots,x_n\}$中$x_i$在有序序列$\{x_1,x_2,x_3,\cdots,x_n\}$中的位置编号，形成置换地址集合T＝$\{t_1,t_2,\cdots,t_n\}$，其中$t_i \in T, i=1,2,\cdots,N$；

（5）、按置换地址集合$\{t_1,t_2,\cdots,t_n\}$对图像的第1行象素进行置换，同时将其第i行象素进行置换，同时将其第i列象素置换至第t_i列，i=1,2,…，N；

（6）、置$x_1=x_N$，对2到M行，重复步骤（2）到步骤（5）。

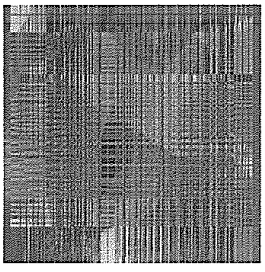
3．2 解密算法

对给定的密匙（迭代初始值x_1），可采用类似置乱的步骤，即只需将其步骤（5）改为：按置换地址集合$\{t_1,t_2,\cdots,t_n\}$对图像的第1行象素进行置换，同时将其第t_i列象素置换至第i列（i=1,2,…，N）即可实现图像的解密。

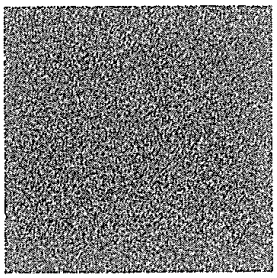
3．3 计算机运行结果

下面的7个图是利用上面基于排序变换的混沌图像行置乱算法对灰度图像进行置乱和解密后的图像。本实验采用Rossler映射，其置乱密匙初值为0.3，图1是Lena原图。图2是用基于排序变换的混沌图像置乱算法对其置乱后的图像，由该图可以看出，置乱后的图像已不能看出原图像的任何轮廓。图3是加密的最终效果图。图4是解密密匙为0.3001解密出来的图像，结果表明，只要密匙稍微不同，就无法解密出原图像，说明其加密效果是很明显的。图5是解密错误时，灰度值替代后的图，可以看出它与置乱后的图像相差很大，根本看不出有任何的共同点或联系。图6是密匙正确时解密出来的图像，由该图可见，解密图像和原始图像完全相同。图7是解密正确时，灰度值替代后的图，可以看出，解密正确时，它是和开始置乱后的图像（图2）是完全一样的。

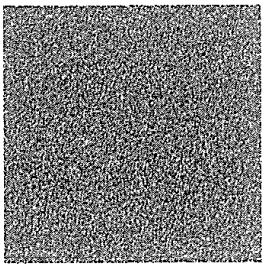
1、原始图



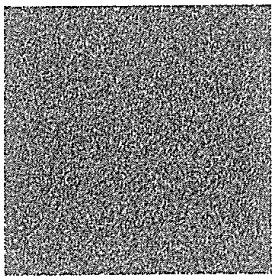
2、置乱后的图像



3、加密后的图像

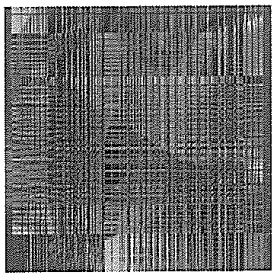


4、解密错误的图像



5、解密错误时灰度值替代后的图

6、解密正确后的图像



7、解密正确时灰度值替代后的图

4、结论

本文给出一种基于排序变换的混沌图像置乱算法，该算法克服了普遍混沌量化图像置乱算法时间复杂度较高和需要对混沌轨道的概率分布有先验知识等缺陷，这不仅方便了混沌置乱算法混沌系统的选择，而且在置乱的速度上也有很大提高。另外，由于排序变换的强不规则性，还增加了算法对混沌映射初始值的敏感度与置乱的复杂度，从而使得新的混沌图像置乱算法具有较高的安全保密性能和足够大的密匙量。通过对新算法置乱性能的统计分析结果表明，该算法不仅具

有良好的置乱性能，还可以有效的保障加密图像的安全，在不知道精确密匙的情况下，无法解密出正确的图像。实验结果和评价表明，文中给出的加密方法是可行的，加密效果良好，密匙空间大，安全性较高，能够有效抵抗盗版人员的非法“攻击”。但是这种算法也有它一定的局限性，就是其循环的次数过多，从而导致运行的速度较慢，在某种程度上影响了其效果，所以在这方面的内容及方法还有待提高。

参考文献

1、李鹏、田东平　基于超混沌序列的数字图像加密算法　微电子学与计算机[J] 2008，25(3)：4-7.

2、蚁秋芸 一种基于 logistic 混沌序列的图像加密技术

3、刘向东、焉德军、朱志良、王光兴 基于排序变换的混沌图像置乱算法 大连民族学院非线性信息技术研究所、东北大学信息科学与工程学院 沈阳

4、韩飞、车晶、郑伟、房春光　一种基于数字混沌的图像加密算法研究

5、刘和松　数学实验报告之一 —— Rossler 方程

6、Zhang Yong-Hong, Kang Abashing, Zhang Xue-Feng. Image encryption algorithm based on chaotic sequence C. IEEE Computer Society, 2006.